생체정보 보호 연구 동향

Technology Trends of the Biometric Template Protection Techniques

반성범(S.B. Pan) 생체인식기술연구팀 선임연구원, 팀장
이경희(K.H. Lee) 생체인식기술연구팀 선임연구원
안도성(D.S. Ahn) 생체인식기술연구팀 선임연구원
정용화(Y.H. Chung) 고려대학교 컴퓨터정보학과, 교수
이남일(N.I. Lee) (주)테스텍 책임연구원, 상무

21세기를 맞이하면서 정보통신 기술의 발전과 인터넷 이용 확산 등으로 사용자 인증이 중요한 문제로 대두되고 있다. 패스워드 또는 PIN을 이용한 사용자 인증 방법이 현재까지 널리 쓰이고 있으나 타인에게 노출되거나 잊어버리는 등의 문제점이 있다. 이러한 문제를 해결하기 위하여 개인의 고유한 생체정보를 이용한 주요 정보 보호 및 사용자 인증 등의 연구가 활발히 진행되고 있다. 그러나, 이러한 생체인식 기술을 대규모 응용에 적용하기 위해서는 생체정보의 안전한 저장/전송/처리 등 생체정보 보호에 대한 연구가 필수적이다. 본 고에서는 이러한 생체정보 보호와 관련된 연구 동향을 소개한다.

I. 서 론

21세기 정보의 시대는 인터넷 보급 등으로 인하여 원하는 정보를 수집, 분석, 가공 등이 편리하게 되었다. 그러나 인터넷을 이용하여 글로벌 네트워크가 형성되어 편리하게 수집, 분석 및 가공한 개인의 중요한 정보가 타인에 의해 도용되거나 파괴되는 심각한 문제가 제기되고 있다. 이는 개인의 정보만이 손실되는 것이 아니라 국가의 중요 정보와 전자상거래 등의 경제 활동에 필요한 정보도 손실되는 현상이 발생되고 있는 현실이다. 그러므로 현재까지 사용되고 있는 사용자 패스워드 또는 PIN(Personal Identification Number)만을 이용한 사용자 인증 방법으로는 개인, 산업, 국가의 중요 정보를 안전하게 보관할 수 없는 실정이다. 이러한 문제를 해결하기 위해 최근 들어 개인의 고유한 생체정보인 신체적 또는 행동학적 특징에 따라 사람들의 신원을 확인하는 바이오메트릭 즉, 생체인식 기술이 대두되고 있다.

미국 Washington DC에 있는 Biometric Consortium에서는 생체인식을 “자동화된 특정 개인의 소추된 특성을 인증하거나 신분을 인식하기 위해, 측정 가능한 특성 또는 개인의 특징을 연구하는 학문”으로 정의하고 있다. 이러한 생체정보를 이용한 생체인식의 예로는 지문, 음성, 얼굴 모양, 홍채 패턴, 손의 형태, 손등의 정맥 분포 등 아주 다양하며, 이들은 신체의 일부분이거나 개개인의 행동 특성을 반영하므로 잊어버리거나 타인에게 대여 혹은 도난 복사가 되지 않는다. 즉, 타인이 지문 혹은 홍채 패턴을 훔쳐갈 수 없고 개인은 지문이나 홍채 패턴 등을 망각할 수 없으며, 집에 두고 올 수도 없다는 것이다. 그러므로 안전한 정보보안을 위한 분야로 활발하게 연구가 진행되고 있다[1],[2].

그러나 생체인식 기술이 이러한 장점이 있지만 사용자 인증을 위해 저장된 생체정보가 타인에게 도

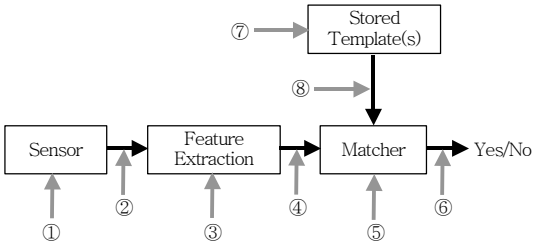
용된다면 패스워드나 PIN과 달리 변경이 불가능하므로 심각한 문제를 일으킨다. 생체정보의 안전한 보관을 위해 최근에는 보안토큰(스마트카드 또는 USB 토큰), PDA 등의 개인기기에 저장하는 연구도 활발하지만, 원격 인증 분야 등에서는 완벽한 보안을 제공하지 못한다. 생체인식 기술이 도어락, PC 보안 등 standalone형 소규모 응용에 성공적으로 적용됨에 따라 다음 단계인 전자정부/전자거래 등 네트워크를 이용한 원격 응용에 적용되기 위해서는 생체정보 보호/관리에 대한 기술 연구가 필요한 실정이다. 또한 네트워크를 이용한 비대면 응용에 적용되기 위해서는 개인의 프라이버시 보호를 위한 생체정보의 안전한 저장/전송/처리 기술이 필요하다. 그리고, 생체정보의 상호운용성 보장을 위한 표준화 작업이 급진전되고 있으므로, 생체정보 오남용에 의한 피해를 막기 위한 연구가 필요하다.

언급한 것과 같이 원격응용을 위한 기존의 비밀번호 보호/위변조 탐지/대응 기술에 상응하는 생체정보 보호/관리 기술 개발이 필요하므로, 본 고에서는 생체정보를 이용한 인증 시스템의 취약점을 분석하고 이의 해결 방안인 질의/응답 프로토콜 기술, 생체정보 위변조 탐지 기술, 응용별로 변형된 생체정보 생성 기술 및 자유로운 생체정보 폐기를 위한 생체정보 변형 기술의 최근 연구 동향을 설명한다.

II. 생체인식 시스템의 취약점 분석

(그림 1)은 전형적인 생체인식 시스템에서의 가능한 공격포인트를 보여주고 있는데 이를 간단히 살펴 보면 다음과 같다.

① 사용자로부터 신호를 얻는 부분으로, 센서에 가짜 지문이나 복사한 서명, 얼굴 마스크 등을 이용하는 경우이다.
② 미리 저장해둔 생체 신호를 다시 사용하는 경우로, 센서를 바이패스(bypass)하고 지문의 복사본이나 오디오 신호를 단자를 통하여 전송한다.
③ 침입자가 원하는 특징을 생성하도록 트로이 목마 등을 이용하여 특징 추출단을 공격한다.
④ 생체인식 시스템의 특징 표현법을 알고 있을 때 이를 임의로 변경하는 경우로, 특징추출과 정합이 한 단계로 이루어지면 어느 정도 해결할 수 있으나, 인터넷으로 특징점이 전송되는 경우에는 TCP/IP에 대한 스누프(snoop)를 통하여 패킷을 변경할 수도 있다.
⑤ 정합하는 자체를 공격하여 미리 선택된 정합 결과가 나오도록 하는 경우로, 아무리 정합알고리듬이 정확하더라도 원하지 않는 결과가 나오게 된다.
⑥ 템플릿이 저장된 데이터베이스를 공격하여 저장된 템플릿을 변경하는 경우로, 특히 템플릿이 분산 저장된 경우에는 그 중에 일부 혹은 전체를 변경함으로써 타인수락률이나 본인거부율이 높아지는 현상을 초래할 수 있다.
⑦ 저장된 템플릿이 전송 채널을 통해서 정합단으로 전송될 때 채널을 공격하는 경우로, 전송되는 데이터를 가로채어 다른 형태로 변경함으로써 상이한 정합 결과를 초래한다.
⑧ 최종 판결을 공격하는 경우로, 아무리 실제 시스템이 우수하고 정확하다고 하더라도 정합결과가 공격을 당하면 아무런 의미가 없게 된다.



(그림 1) 생체인식 시스템에서 가능한 공격포인트

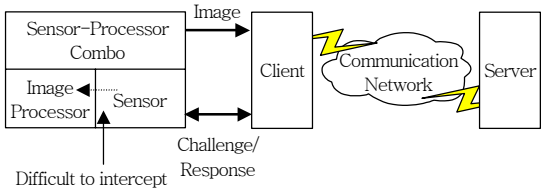
위와 같이 여러 공격포인트가 존재하며, 아울러 이러한 공격을 피해갈 수 있는 방안 또한 강구되어야 한다. ①번 공격포인트에 대한 부분은 현재 일본 등에서 다각적으로 검토 연구되고 있다[3]. 실제 손가락을 이용한 방법 뿐 아니라 잔상 지문을 이용해서도 유사한 방법으로 가짜 지문을 만들 수 있다. 따

라서 “가짜지문 여부를 어떻게 판단할 것인가?”라는 문제에 봉착하게 된다. 이의 해결 방법으로는 소프트웨어적 접근법과 하드웨어적 접근법이 있다. 소프트웨어적인 방법으로는 지문의 경우 땀샘, 얼굴의 경우 머리의 움직임, 홍채의 경우 눈의 움직임 등을 이용한다. 하드웨어적인 방법으로는 지문의 경우 손가락의 온도와 맥박을 측정하거나 전기적 특성을 이용하는 방법도 가능하다. 이들 방법을 잘 이용하면 완전하지는 않지만 센서단에서의 공격은 어느 정도 막을 수 있다. 암호화된 채널을 이용하면 공격포인트 ④번에서의 원격공격은 막을 수 있다. 그리고 공격 포인트 ⑤, ⑥, ⑦에 대한 간단한 방어책은 정합단이나 데이터베이스를 안전한 곳에 설치하는 것이다. 일반적으로 ⑧번의 경우는 암호화를 통해서 공격을 막을 수 있다. 지금부터는 이들에 대한 예를 통해서 가능한 공격을 이해하고 대응방법에 대해서 논하기로 한다.

III. 생체정보 보호/위변조 탐지 기술

1. 질의/응답 프로토콜 기술

생체인식 시스템에 대한 손쉬운 공격은 (그림 1)에서 지문 센서로부터 나오는 신호를 공격하는 것이다(공격포인트 ②). 이러한 공격을 방지하기 위한 방법이 변형된 질의/응답(Challenge/Response) 프로토콜 기술이다[4]. 기존의 일반적인 질의/응답 방법에서는 사용자에게 어머니의 처녀시절의 이름을 요구하는 등의 질의나 특수목적의 계산기와 같은 물리적인 장치에 대한 질의를 요구하는 데 근거를 두고 있었다. 여기서는 사용자의 ID만 확인하는 것이 아니라, 센서의 정보까지 확인한다. 센서는 질의에 반응을 할 수 있는 충분한 능력을 가지고 있다고 가정한다. 물론 기존의 암호화 기술이 수학적으로는 충분히 강력한 기능을 가졌다고 할 수는 있지만 수많은 센서에 대한 비밀 키를 관리 운영해야 한다는 어려움이 있다. 더구나 암호화 방법은 시그널에 대한 liveness 체크는 불가능하다. 본 방법의 특징은 질의



(그림 2) 질의/응답 프로토콜

내용에 대한 응답이 센서로부터 취득한 생체정보와도 연결되어 있다는 것이다. 그러므로 질의를 바꾸기만 하면 획득한 영상이 질의가 발생한 이후에 만들어진 것인지를 알 수가 있다. 응답이 생체정보에 의해서 만들어지기 때문에 반응이 일어난 후의 다른 가짜 생체정보에 대해서는 구별이 가능하다.

(그림 2)는 질의/응답 프로토콜 시스템의 전체 흐름을 보여 주고 있다. 트랜잭션이 처음에 사용자 단말기나 서버에서 발생한다. 처음에 서버는 트랜잭션이나 서버를 위한 랜덤 질의 코드를 만든다. 물론 센서는 사람의 liveness를 검사할 수 있으며, 서버는 보안성을 유지한다는 가정이 있어야 한다. 그러면 클라이언트 시스템은 이 질의를 센서에 보내고 센서는 새로운 생체정보를 취득하고 질의 내용에 대한 응답을 만든다. 물론 센서에는 프로세서가 내장되어 있다고 가정하며, 센서와 프로세서가 하나의 칩으로 구성되어 있으면 좀 더 높은 보안을 제공할 수 있다.

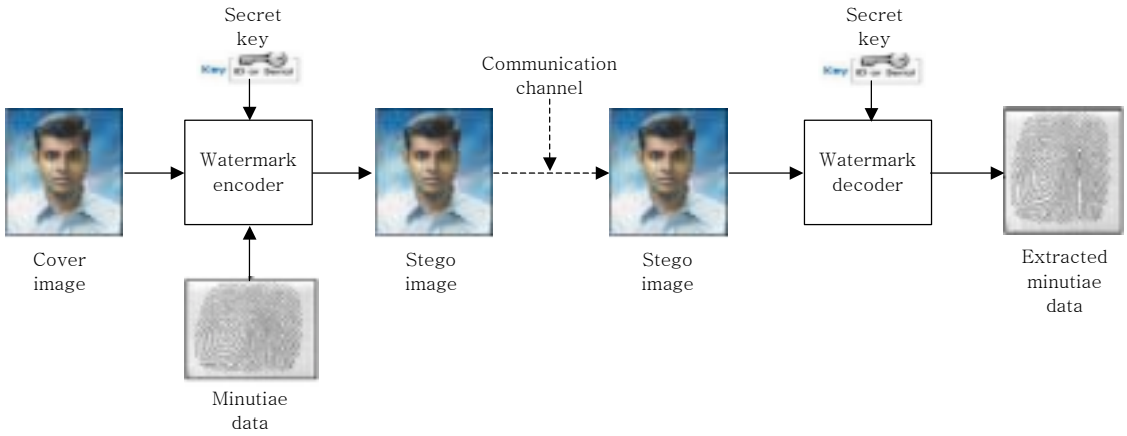
지문인식 시스템을 이용하여 질의/응답 프로토콜을 설명하면 다음과 같다. 지문 센서에 대한 외부의 공격을 막기 위해 지문 센서의 동작을 서버에서 제어하게 되는데, 센서의 제어를 위해 서버에서는 pseudorandom 함수를 클라이언트에 전송해주며, 프로세서가 내장된 센서는 이 함수를 이용해 서버에 응답 코드를 전송하게 된다. Pseudorandom 함수로 사용할 수 있는 함수는 매우 많으며, 예로 서버에서 “3, 10, 50” 이란 명령을 클라이언트에게 하게 되면, 센서는 현재 입력하려는 사용자의 지문 영상으로부터 3, 10, 50번째 픽셀 값을 취득하여 일정한 규칙에 따라 새로운 코드 “133, 92, 176”을 만든다. 이런 값을 응답 코드라고 하며 이것을 서버로 전송한다. 결론적으로 질의/응답 프로토콜 기술은 센서에

프로세서가 하나의 칩으로 구성되고 트랜잭션 서버가 안전하다면 질의 변경만으로 생체정보의 live-ness 검증과 생체정보의 만들어진 시점을 알 수 있게 한다. 그러므로 (그림 1)의 공격 포인트 ②에 대한 대응이 가능하다.

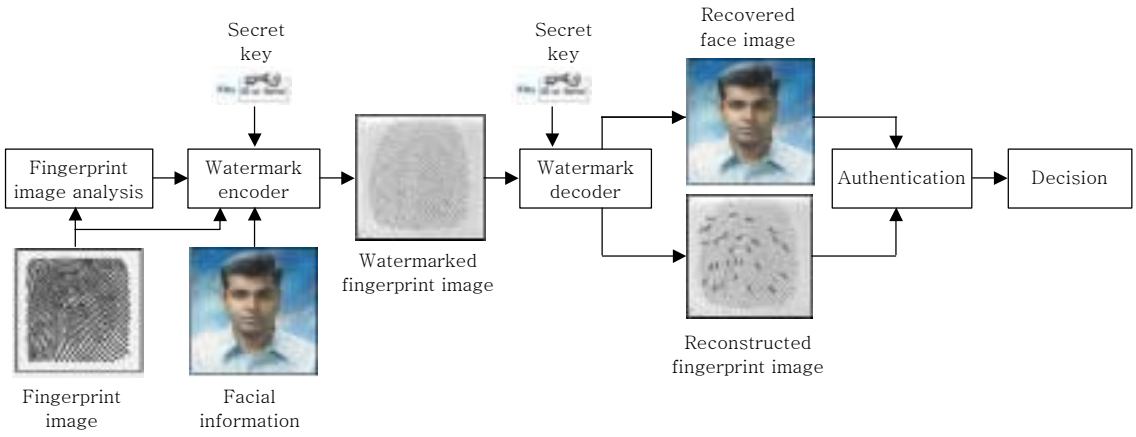
2. 워터마킹

생체정보의 위변조 방지를 위해 생체정보에 추가정보를 끼워넣는 워터마킹 기법을 이용하는 것도 고려할 수 있다. 만약, 임베딩 알고리듬이 알려지지 않는다면, 서비스 공급자는 표준 워터마킹 기술을 사용해 전송될 지문 영상의 안전성을 보장할 수 있을 것이다. 즉, 공격포인트 ④, ⑥, ⑦에 대한 대비책으로, DB에 저장된 지문 영상의 위변조를 막거나 전송전에 워터마크를 삽입하고 수신단에서 워터마크를 확인함으로써 지문 영상을 안전하게 전송할 수 있다.

영상에 대한 워터마크를 통해 데이터를 은닉하는 기술은 많이 알려져 있다. 그러나, 대부분의 워터마크 기술들은 저작권 등을 위한 연구였으며, 인증에 대한 연구는 거의 없었다. 최근 발표된 지문 영상을 위한 fragile 워터마킹 기법[5]에서는 영상 도메인에서 워터마크를 첨부할 때 정확성을 조사하였고, 국부적인 블록 평균에 근거한 semi-unique key를 이용하여 지문이나 얼굴 영상의 위변조를 검출하는 연구[6]도 발표되었다. 또한, 지문 특징추출 전과



(그림 3) 지문 은닉



(그림 4) 얼굴 은닉

후에 워터마크를 삽입하는 방법에 대한 연구[7]에서는 지문특징이 신원 확인을 위해 사용되기 때문에 삽입된 워터마크가 지문 영상의 특징을 변경하지 않도록 제안되었다.

최근에는 얼굴 영상에 지문 특징[8] 또는 지문 영상에 얼굴 특징[9]을 은닉하여 지문/얼굴 호스트 영상의 위변조 여부를 확인함과 동시에 은닉된 얼굴/지문 특징을 추가로 이용하여 멀티모달 생체인식 시스템에 대한 연구도 발표되었다. 예를 들어, (그림 3)은 얼굴 호스트 영상에 지문 특징을 워터마크로 사용한 워터마킹 시스템을, (그림 4)는 지문 호스트 영상에 Eigen Face Coefficient를 워터마크로 사용한 워터마킹 시스템을 보여준다.

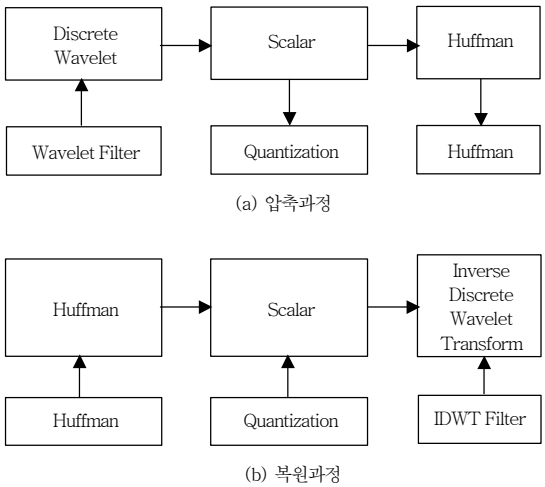
3. WSQ 기반 데이터 은닉

다음은 앞서 언급한 워터마킹의 특별한 경우로, 압축된 지문영상에 대한 데이터 은닉 기법에 대하여 설명한다. 일반적으로 웹 기반이나 온라인 전송 시스템에서는 전송 대역폭의 제한 때문에 압축하지 않는 상태로 영상을 서버로 보내는 것이 바람직하지 않다. 예를 들어서, 512×512 픽셀의 256 그레이 영상(256kbyte)을 53kbaud의 전송 속도로 전송하면 약 40초가 소요된다. 불행히도, 대부분의 표준 영상 압축 방식(JPEG 등)들은 고주파 성분이 왜곡되어 지문의 융선 구조가 왜곡된다는 문제가 있다. 따라서, 영상 왜곡을 최소화한 WSQ(Wavelet Scalar Quantization) 영상 압축을 FBI에서 제안하였으며, 지문 영상 압축 방식으로 사실상 표준화되어 사용되고 있다.

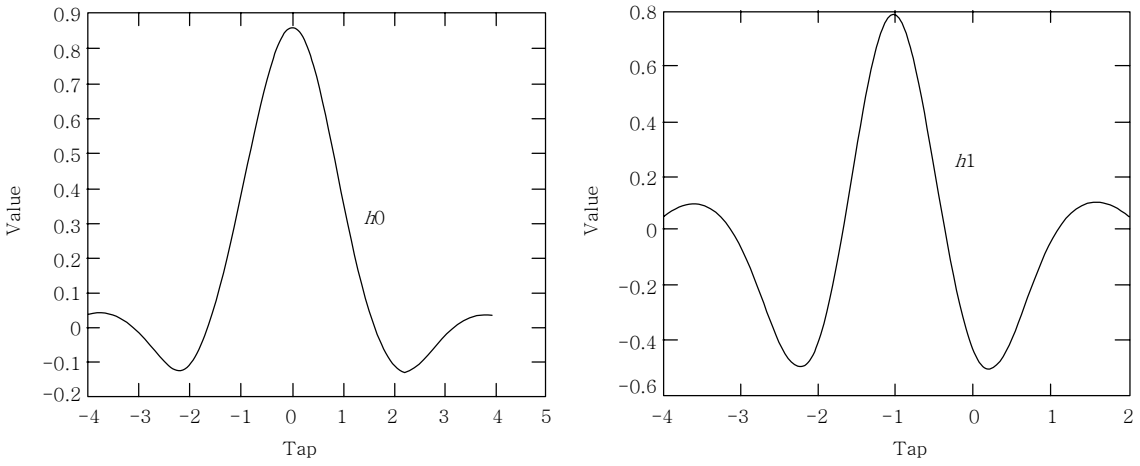
일반적으로 압축된 영상은 사용자의 PIN을 대신해서 표준 암호화 채널을 통해서 전송된다. 그러나 개방된 압축표준 때문에 인터넷을 통해서 WSQ로 압축된 영상을 전송하는 것은 그렇게 안전하다고 할 수 없다. 만약에, 압축된 지문 영상이 전송단에서 자유롭게 가로챌 수 있다면, 복원 소프트웨어를 사용해 지문 영상을 자유로이 읽을 수 있으며, 결과적으로 신호를 저장하여 재사용이 가능해진다(공격포인트 ②).

상업용으로 사용되는 온라인 지문인식 시스템에서는 replay attacks으로부터 전송정보를 보호할 수 있어야 한다. 이러한 목적으로, 서비스 공급자는 전송될 지문 영상들에 대해 매번 서로 다른 인증 스트링(verification string)을 부여한다. 즉, 전송하기 전에 전송될 지문 영상에 스트링을 첨부한다. 그리고, 서비스 공급자가 받은 영상은 복원되며 one-time verification string을 검사하여 올바른 지문 영상인지 확인한다. 여기서 인증 스트링은 복원 영상에 영향을 최소화하는 방향으로 설정되어야 한다. 또한, 이 스트링은 고정된 장소에 숨겨져서는 안된다. 고정된 위치에 둘 경우 해킹을 당할 염려가 있기 때문이다. 따라서 이미지 자체의 구조를 이용해서 다른 장소에 위치시켜야 한다. 다음 예에서 지문 영상 압축 과정에서 워터마크를 첨부하는 방법을 중심으로 기술하고자 하는데, 웨이블릿 얼굴압축 이미지와 같은 기타 다른 생체 기술에도 쉽게 적용될 수 있다. 이 정보 은닉(information hiding) 기술은 WSQ 지문 이미지 송신단과 수신단의 결합으로 동작한다. 지문 영상의 WSQ 송신단과 수신단에서 정보 은닉하는 과정을 (그림 5)에 나타내었다.

WSQ 압축은 크게 두 가지 과정으로 구성되어 있다[10]. 첫번째 과정은, 입력 영상을 DWT(Discrete Wavelet Transformation) 필터에 근거하여 완전



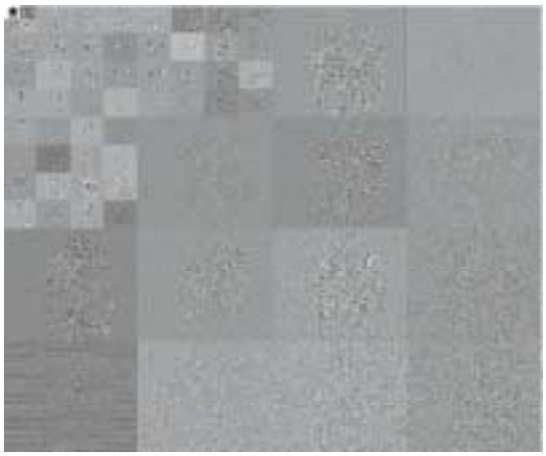
(그림 5) WSQ 알고리듬



(그림 6) FBI WSQ 표준 필터

(a) 원 지문 영상 (b) 복원 지문 영상

(그림 7) WSQ 데이터 은닉 결과



(그림 8) 64 서브밴드 영상

복원(perfect reconstruction)이 가능한 64 spatial frequency filter bank로 분해하는 것이다. FBI에서 표준으로 사용되고 있는 두 필터를 (그림 6)에 나타내었다. 이들 필터를 적용한 지문 영상 (그림 7)에 대한 64 서브밴드 영상은 (그림 8)과 같다.

WSQ 압축의 두번째 과정은 양자화 처리(quantization process)이다. 각각의 서브밴드를 일정한 스칼라 양자화(scalar quantization)를 이용하여 작은 정수값인 DWT 계수들로 정한다. 각 주파수 밴드에는 두 가지 특징(The zero of the band(Z_k)와 the width of the bins(Q_k))이 있는데, 이를 정보 손실없이 압축하기 위해서는 두 가지 파라미터들의 값을 적절히 선택해야 한다. 각 주파수 밴드의 Z_k, Q_k는 수신단에 전달된다. 그리고, 각각의 밴드들은 3개로 군집화하고, 각각의 군집 블록에 있어서 정수 계수들은 테이블에 의해 0~255 사이의 값으로 재할당된다.

데이터 은닉 알고리듬은 마지막 변형 전에 양자화된 인덱스에 의해서 동작되며 메시지 크기는 영상에 비해 매우 작다. 그러나, 허프만 코딩 특징과 테이블은 변하지 않는다. 실제 영상 송신 과정에서 메시지를 숨기기 위해서는 다음과 같은 4 단계를 거쳐서 처리된다.

1단계: 위치 후보자 집합 S의 선택

부분적으로 양자화된 정수 인덱스가 주어지면 이 단계에서는 모든 가능한 계수의 인덱스를 모은다. 작은 변화에도 영상의 많은 부분에 영향을 주기 때

문에, 일반적으로 저주파 대역에서의 모든 부분은 제외한다. 고주파 대역에서는 큰 계수를 가졌을 경우에 후보자로 선정한다. 여기서는 일반적인 경우를 생각해서 0~255 사이의 정수 계수가 주어지면, 실제 중요한 정보가 있는 계수 범위(예, 107~254)를 정하여 후보 집합 S를 정한다.

2단계: RNGS(Random Number Generation Seed)의 생성과 위치 선택

후보 집합 S의 모든 계수를 입력 변수로 사용하여, 이것의 조합으로 후보 집합 S 중 하나의 밴드를 선택하는 함수를 정의한다(seed selecting algorithm). 그리고, seed selecting algorithm에 의해 선택된 하나의 주파수 밴드를 메시지 은닉 밴드로 설정한다.

3단계: 선택된 위치에 메시지 숨김

먼저 숨겨져야 할 메시지를 일련의 비트(bit)로 변환한다. 각각의 비트는 seed가 되는 RNG(Random Number Generator)에 의해서 선택된 부분과 일치되게 선택한다. 만약에 선택된 위치가 이미 사용중이라면 다음 생성된 위치가 선택된다. 앞에서 RNG에 의해 선택된 주파수 밴드에 지문영상의 authentication을 위한 메시지를 첨부한다.

4단계: 이미지에 비트 첨가

선택사양으로 모든 하위 비트는 사용자 명령어 항목으로 압축된 비트 스트링에 첨가된다. 그러므로 이 하위 비트는 숨겨진 메시지와는 아무런 관계를 갖지 않는다. 복구과정이 포함되어 있다면 수신단은 메시지를 재구성하는 동안 하위 비트를 선택적으로 복원할 수 있다. 이렇게 함으로써 메시지가 첨부되어 있음에도 불구하고 원래의 압축과 거의 유사한 이미지를 만들어내게 된다. 실제 메시지가 첨가됨으로 인한 차이는 인식할 수 있을 정도가 되지 않으며, 후속적인 처리 과정이나 개인인증의 기능에 전혀 영향을 주지 않는다. (그림 7)에 위와 같은 결과로 만들어진 이미지를 원 이미지와 비교해주고 있다.

이와 같은 처리 과정을 이용함으로써 아주 특별한 수신단만이 압축된 영상으로부터 위치를 알고 해당하는 메시지를 추출할 수 있다. 즉, 수신단에서 RNG를 가지고 있다면, 메시지가 은닉되어 있는 주파수 밴드로부터 은닉 메시지를 확인할 수 있다. 이 메시지는 인증서나 개인 ID와 같이 혼용하여 사용할 수 있다. 만약, 비트열이 메시지를 갖고 있지 않다거나 다른 형태를 가질 경우에는 이 특수한 수신단은 특별한 메시지 추출에 실패하여 이 영상을 거절하게 된다. 동일한 많은 알고리듬이 실제 구현됨에 있어서는 서로 다른 RNG를 사용하기 때문에 큰 노력이 없이도 모든 구현을 유일하게 만들 수 있다. 또한, 하나의 결과가 다른 수신단의 결과와는 부분적으로도 같을 수 없다. 따라서 한 버전을 크래킹 하더라도 다른 버전에서는 사용이 불가능하다. 이와 같은 방법을 사용하면, 해커가 센서로부터 전송되는 압축 지문영상을 가로채더라도, 데이터 은닉 알고리듬을 가지고 있지 않다면 압축 지문영상의 재사용이 불가능하게 된다.

IV. 생체정보 관리 기술

생체정보의 장점인 “시간이 경과하여도 변형되지 않고 유일하다는 특징”으로 인하여 생체정보가 유출이 되면 전체 생체인식 시스템이 동작하지 않게 된다. 최근에는 이러한 문제를 해결하기 위하여 취득한 생체정보를 전송, 저장, 인식과정에서 사용하지 않고, 역변환이 불가능한 변환을 이용하여 변형된 생체정보를 인식과정에 사용하여 생체정보 유출에 대비한 Cancelable Biometrics 기술이 소개되었다. 또한, 응용별로 생체정보를 생성할 수 있는 Application Specific Biometric Template 기술도 제안되었다.

1. Cancelable Biometrics

신용카드 인증, 은행 ATM 접근 등과 같은 큰 시장에 생체 인식 제품을 적용하려면 트랜잭션에 대한

보안뿐만 아니라 그 이상의 부가적인 상황이 발생하게 된다. 이것은 가능성이 있는 개인 프라이버시의 침해에 대한 부분이다. 이름이나 생년월일 등과 같은 개인 신상에 대한 정보 뿐 아니라 사용자는 지문, 얼굴, 홍채 등의 개인 신체의 일부에 대한 정보가 도난당할 수 있다는 것이다. 이들 영상이나 다른 생체 정보는 다양한 데이터베이스에 디지털 형태로 저장된다. 이렇게 디지털로 저장된 데이터가 범죄 수사와 같은 수사기관이나 은행이나 기타 인터넷을 이용하는 다른 상업적인 사업체에서 공유될 수 있다는 사실이다.

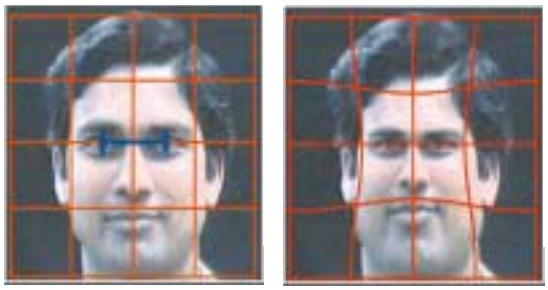
우리 사회에서 개인에 관한 신상 및 신체의 일부에 대한 디지털화된 정보가 점차 상당한 속도로 증가하고 있다는 사실에 귀를 기울이게 된다. 이렇게 모아진 데이터가 많은 응용분야에서 사용되고 있으며 이들에는 의료기록이나 신체정보도 포함되고 있다. 이로 인하여 다양한 데이터베이스로부터의 데이터를 공유하고 상호 협력할 수 있다는 것 또한 큰 관심사가 되지 않을 수 없다. 생체 정보와 관련해서는 개인 회사에서 모아진 데이터가 범죄 수사용으로 사용되어질 수도 있다는 사실이다. 한 사람의 생체정보가 주어지면 이것은 다시는 바꿀 수 없다는 사실 때문에 더욱 더 큰 관심을 불러 일으키고 있다. 생체정보가 개인인증용으로 사용되어질 수 있는 가장 큰 이유 중의 하나는 시간의 흐름에도 크게 변하지 않는다는 것이다. 만약에 신용카드 번호에 의한 피해가 발생한 경우 해당은행에서는 사용자에게 새로운 신용카드 번호를 부여함으로써 문제를 최소화할 수가 있다. 그러나 생체정보의 경우에는 데이터가 도용되고 있음에도 불구하고 바꿀 수 없다는 문제가 있다. 이와 같은 위험을 최소화하기 위해서는 생체정보를 취소할 수 있는 시스템이 되어야 한다. 일반적으로 이를 “Cancelable Biometrics”[11]라고 하는데, 선택한 함수를 이용하여 의도적이면서도 반복 사용가능한 생체정보의 변형을 할 수 있다는 것이다. 즉, 매번 등록이나 인증 시에 생체정보가 나타나면 같은 방법으로 정보를 변형하는 것이다. 이와 같은 방식으로 매번 등록 시마다 서로 다른 변형함수를 사용함으로써 크로스 매칭이 불가능하도록 하는 것이다. 더구나 변형된 생체정보가 도용되었을 경우에도 재등록을 위해 다른 변수를 사용함으로써 변형함수를 간단하게 바꿀 수 있다. 즉, 새로운 사람으로 인식되는 것이다. 일반적으로 변형함수는 noninvertible하게 만들어서 사용한다. 이렇게 함으로써 변형함수가 알려지거나 심지어는 변형된 생체정보가 알려지더라도 변형되기 전의 생체정보는 복구가 불가능하다.

가. Distortion Transform

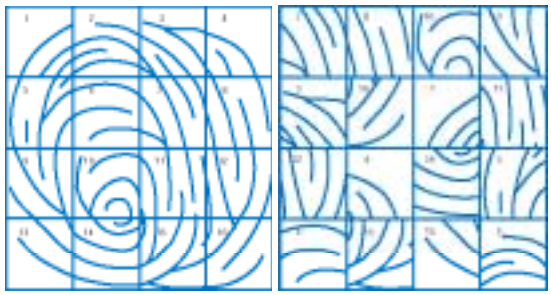
이와 같은 방법에서는 변형함수가 signal domain이나 feature domain에서 적용될 수 있다. 즉, 생체정보를 획득한 바로 직후에 직접 변형을 할 수도 있고 아니면 평상시처럼 시그널을 처리한 후 추출한 특징을 변형하는 방법도 가능하다. 가장 이상적으로는 변형함수가 반드시 noninvertible해서 다양한 기관이나 회사 등에서 저장된 변형된 데이터를 이용해서는 원 영상을 복구할 수가 없어야 한다. Signal 차원에서의 변형 함수로는 grid 모핑(morphing)이나 block permutation 등을 들 수가 있다. 이렇게 변형된 영상은 원 영상과 성공적으로 매칭될 수 없으며, 같은 영상으로부터 다른 변형 파라미터에 의해 변형된 영상과도 매칭될 수가 없다. 변형 가능한 템플릿 방법을 사용하게 되면 이와 같이 원래의 생체정보 보호 측면에서 안전한 매칭을 수행할 수 있는 장점이 있다.

Signal domain에 대한 변형의 예로서 (그림 9)는 영상 모핑에 의한 변형을 보여주고 있다. 왼쪽의 원 영상은 얼굴 위에 그리드를 올려놓은 것처럼 보인다. 오른쪽의 경우에는 동일한 얼굴에 대한 모핑된 결과를 보여주고 있다. 다른 방법으로서 (그림 10)과 같이 원 영상에 대하여 나누어진 블록영역을 랜덤하게 위치를 바꾸어주는 방법이 있을 수 있다.

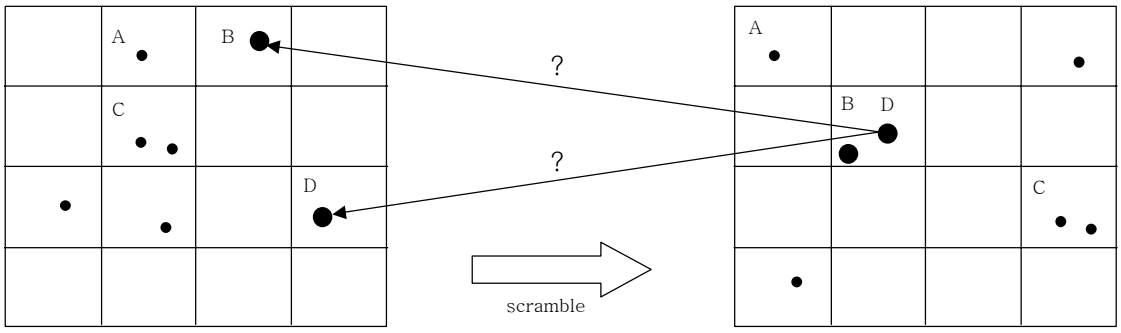
Feature domain 상에서의 변형 예로는 특징점의 Random, Repeatable perturbation set을 들 수가 있다. 이것은 원영상과 동일한 물리적인 공간에서 이루어질 수도 있으며 차원을 높임으로써 보다 높은 보안 강도를 얻을 수도 있다. (그림 11)은 feature



(그림 9) 영상 공간에서 영상 모핑에 의한 변형 예



(그림 10) 영상 공간에서 재배열을 통한 변형 예



(그림 11) 특징 공간에서 특징 벡터 교반(perturbation)에 의한 변형 예

perturbation에 근거한 변환을 보여주고 있다. 여기서 왼쪽에 있는 블록은 랜덤하게 오른쪽에 있는 블록에 사상되고 있다. 물론 여러 개의 블록이 같은 오른쪽 블록에 사상될 수도 있다. 이와 같은 변형은 noninvertible하기 때문에 변형된 것을 이용해서는 원래의 특징을 찾을 수가 없다. 예를 들어 (그림 11)에서 오른쪽의 포인트 B, D가 어느 블록에서 왔는지는 알 수 없다. 결과적으로 등록 시에 있었던 특별한 정보 없이는 생체정보의 주인이 누구인지를 확인할 수 없다는 것이다. 그러나 변형이 repeatable하게 되기 위해서는 생체 시그널을 변형 전에 어디엔가 저장을 해두어야 한다. 다행히 지문에는 중심점과 삼각주라는 특징이 존재하며 얼굴 인식의 경우는 눈과 눈 사이의 거리 등과 같은 정보를 변형의 힌트로 활용할 수 있다.

나. Feature Domain Transforms

이제 point pattern에 대한 noninvertible한 예를 들어서 살펴보기로 하자. 이와 같은 point pattern은 (1)과 같이 지문의 특징점의 집합으로 표현될 수 있다.

$$S = \{(x_i, y_i, \theta_i), \quad i = 1, \ldots, M\} \tag{1}$$

물론 이 집합은 다른 생체정보(음성의 주파수나 크기)를 나타낼 수도 있다. Noninvertible 함수는 이 집합 S 를 새로운 집합 S'로 변형을 할 수 있으나, 원래 S 는 S'를 이용해서 복구가 불가능하다.

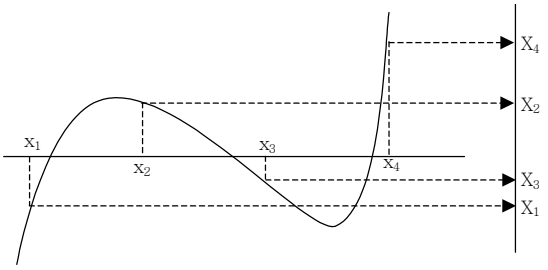
$$\begin{aligned} S &= \{(x_i, y_i, \theta_i), \quad i = 1, \ldots, M\} \\ \rightarrow S' &= \{(X_i, Y_i, \Theta_i), \quad i = 1, \ldots, M\} \end{aligned} \tag{2}$$

(그림 12)는 point set S 의 x 좌표가 어떻게 매핑 함수 $F(x)$를 통해서 $x \rightarrow X$ 로 변형되는지의 예를 보여 주고 있다. 여기서 $F(x)$는 고차원 다항식

$$X = F(x) = \sum_{n=0}^{N} \alpha_n x^n = \prod_{n=0}^{N} (x - \beta_n) \tag{3}$$

으로 표현할 수 있다.

(그림 12)에서 보는 바와 같이 $x \rightarrow X$ 은 1대 1 사상이다. 그러나 $X \rightarrow x$ 방향은 1대 다 사상이다.



(그림 12) Noninvertible 특징 변환 예

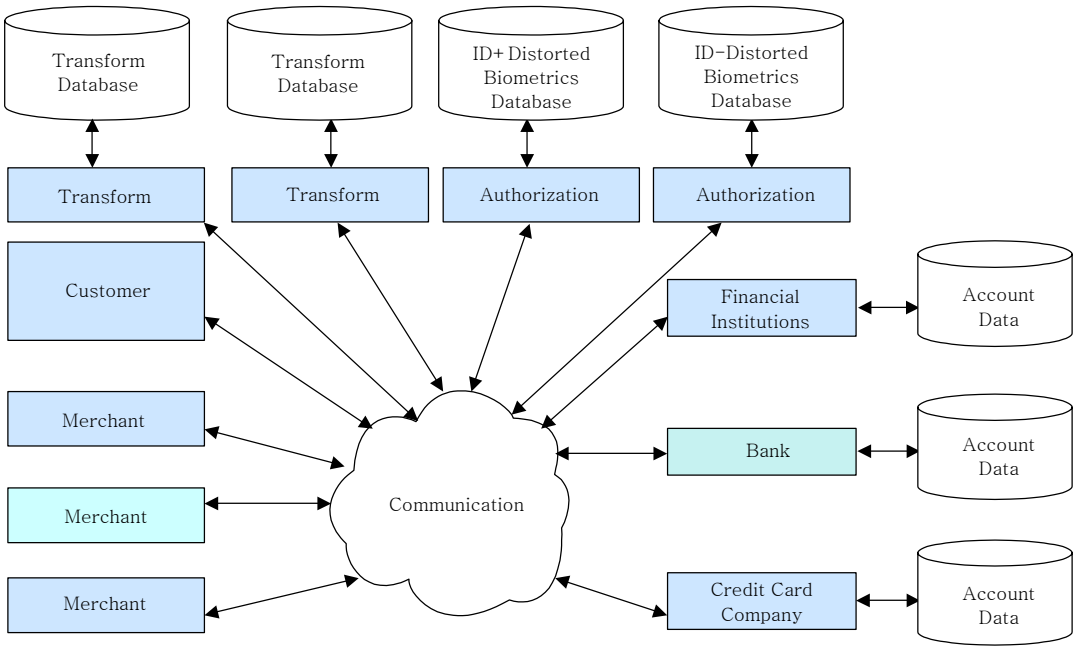
예를 들어서 출력값 중의 하나인 X_1 은 서로 다른 세 개의 입력값 x 로부터 만들어진 것이다. 그러므로 이 함수는 noninvertible 함수라고 할 수 있으며, 원래의 특징인 x 는 X 로부터 복구가 불가능하다.

다. Encryption and Transform Management

생체정보의 변형을 위해서 여기서 사용되고 있는 기술은 시그널이나 영상처리기술을 이용한 단순한 압축과는 엄연히 차이를 두고 있다. 영상압축에 의한 것은 공간 도메인의 특징을 어느 정도의 손실을 감수해야만 하지만, 이 기술은 모든 정보를 보전할 수 있다. 즉, 두 개의 포인트를 사용할 경우 압축 전의 거리는 압축 후 다시 압축을 풀었을 때와는 어느 정도의 차이를 가지고 있다는 것이다. 이와 같은 현상이 distortion transform에서는 발생하지 않는다. 또한 이 기술은 압축과는 또 다른 점이 있다. 암호화의 목적은 원래의 신호를 재생산하는 것인 반면에 distortion transform은 noninvertible한 방법으로 신호를 영원히 감지할 수 없도록 만드는 것이다.

Cancelable Biometrics를 적용하려면 transform 함수나 그의 매개변수, 그리고 인식 템플릿을 저장할 수 있는 장소가 여러 군데 있어야 한다. 이를 고려하면 (그림 13)처럼 동작하는 분산처리 모델의 정립이 필요하다.

(그림 13)에서 "Merchant"가 이 모델에서의 모든 내부 활동이 시작되는 시발점이 된다. Customer ID에 근거를 해서 해당하는 변형함수를 변형함수 데이터베이스에서 가지고 와서 이를 해당 Biometrics에 적용한다. 그러면 그 결과 변형된 Biometrics는 인증을 위해 "Authorization" 서버에 보내지게 되고, 사용자의 Identity가 확인되면 트랜잭션 처리를 필



(그림 13) Cancelable Biometrics에 기반한 인증 분산처리 모델

요로 하는 마지막 국가기관이나 은행, 신용카드 회사 등으로 보내진다.

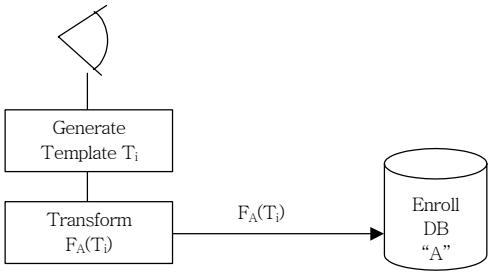
한 사람이 여러 기관이나 여러 가지 서비스를 위해 다양한 서비스를 등록할 수 있다는 것을 고려한다면, 각각의 트랜잭션 단위로 서비스 제공자에 의해서 각각이 독립적으로 인증되어야 함을 알 수가 있다. 마찬가지로 변형함수 역시 인증기관이나 기타 다른 독립적인 기관에서 관리함이 전체 시스템의 보안을 위해서는 필요하다고 볼 수 있다. 아니면 개인의 프라이버시를 위해 개인 자신이 자기 자신의 변형함수를 스마트카드 등에 보관하는 것도 하나의 방법이 될 수 있다. 만약에 카드를 분실하거나 도난당했을 경우에도 이 변형함수를 다른 사람의 생체 정보에 적용한다고 하더라도 큰 충격을 주지는 못할 것이다. 그러나 변형된 함수가 진짜 사용자 자신의 저장된 생체 정보에 적용될 경우에는 그 사람의 저장된 템플릿과의 매칭이 이루어 질 것이다. 이러한 잘못된 사용을 방지하기 위해서는 “Liveness” 여부를 체크하는 시스템의 적용이 필요하다.

2. Application Specific Biometric Template

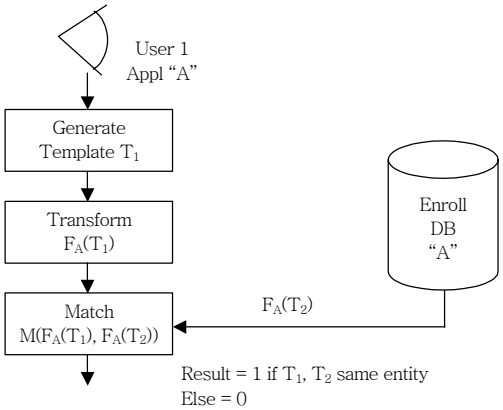
그러나 이러한 Cancelable Biometrics를 구축하는 것도 아직 생각해야 할 여지가 많이 남아 있다. 그중의 하나는 변형함수를 어디에 안전하게 저장하느냐 하는 것이다. 앞에서 언급을 했지만 (그림 13)처럼 서버에 저장하는 경우 서버에 대한 보안이 기본적으로 전제되어야 한다. 아니면 개인이 소유하는 스마트카드 등에 저장 보관하게 하면 보안성 및 프라이버시 문제를 좀 더 확실히 해결할 수 있을 것이다. Signal이나 feature 기반의 distortion transform model 중 어느 것이 더 효과적인지는 뚜렷한 통계적 근거가 아직 없는 상태이다. 때에 따라서는 두 가지를 혼합하여 사용하는 방법도 가능할 것이다. 앞서 언급한 가짜 지문이나 위장 얼굴 등에 대해서 어떻게 처리할 것인가? 즉, 이들을 가지고 변형함수가 있는 데이터베이스에 접근을 하게 되면 해결책을 찾을 수 없다. 또한 한 개의 지문이나 얼굴에 대해서 몇 가지 정도의 함수를 사용할 수 있을까? 마지막으로 이러한 시스템의 경우 에러율은 어떻게 변하는가 등에 대한 연구가 이루어져야 한다. 또한 Cancelable Biometrics 기술은 raw biometric data에 noninvertible 변형함수를 적용함으로써 항상 재사용이 가능하게는 할 수 있으나, 모든 응용분야별로 따로 템플릿이나 데이터를 저장해야 하는 번거로움이 있다. 즉, 한 번 등록된 데이터를 공유할 수 있는 방법은 제공하지 않는다. 각각의 응용분야별로 유일한 포맷을 만들 수 있도록 하고 한 포맷에서 다른 포맷으로의 변환을 가능하도록 해준다면, 매 응용마다 재등록을 할 필요도 없이 사용자의 인정 하에 응용분야간 템플릿을 공유할 수가 있다. 그리고 매칭은 변형된 템플릿에서 이루어지도록 시스템을 설계하면 단순한 Cancelable Biometrics 보다 더 효과적으로 생체정보 관리를 할 수 있다.

최근 응용에 따라 독특하게 변환된 템플릿을 생체 데이터베이스로 저장하는 기법에 관한 연구[12]가 보고되고 있는데, 본 절에서는 이를 자세히 살펴보기로 한다. (그림 14)는 응용에 따라 독특한 변환(transform)을 이용하는 사용자 등록 과정을 나타낸다. 사용자의 생체 정보로부터 표준 포맷인 루트 등록 템플릿(T_i)을 생성한 후, 이를 다시 응용 A의 독특한 포맷으로 변환하여 얻어진 $F_A(T_i)$을 데이터베이스에 등록하는 과정을 나타낸다. 여기서 또한 적절한 소프트웨어 디자인을 이용하여 변환 과정을 템플릿 생성과정에 통합시킴으로써, 어떠한 루트 템플릿의 생성도 없이 직접 변환된 템플릿을 만들 수 있다. 이렇게 하면 루트 템플릿의 가능한 노출도 피할 수 있게 된다.

예를 들어, 응용 A에 관련된 인식 과정은 (그림 15)와 같다. 정합함수 $M(F_A(T_1), F_A(T_2))$는 새로 생성되어 변환된 루트 템플릿과, 응용 A의 데이터베이스 내의 하나 혹은 여러 개의 템플릿들과 비교하는 과정을 수행한다. 만약 응용 A의 템플릿을 응용 B에서 생성된 데이터베이스에 인증하려고 하면 정합 함수는 다른 포맷의 템플릿을 비교하게 되어 결국 항



(그림 14) 등록



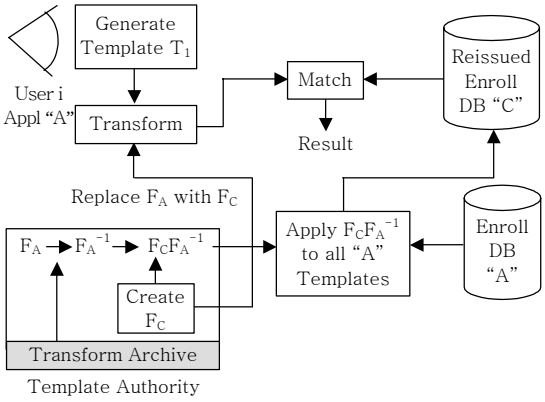
(그림 15) 정합 함수

상 정합되지 않았음을 나타내게 된다.

포맷 변환 방법은 새로운 템플릿을 생성하는 과정에 사용될 수 있는 특성을 갖는다. 다음과 같은 변환 $F_{A,B}$를 정의한다. (4)에서 F_B는 응용 B용으로 생성된 포맷을 나타낸다.

$$\text{Result} = \begin{cases} 1, \text{ if } T_1, T_2 \text{ same entity} \\ 0, \text{ otherwise} \end{cases} \quad (4)$$

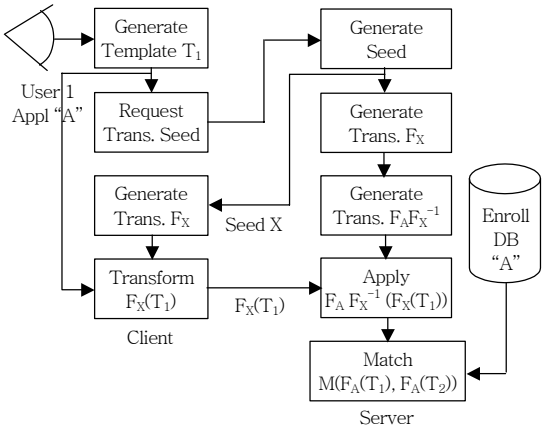
사용자는 데이터베이스 A의 관리자에게 포맷을 바꾸는 변환 $F_{A,B}$ 를 수행하여 그의 등록된 템플릿을 응용 B의 데이터베이스에 이용할 수 있도록 요청할 수 있다. 이러한 과정의 장점은 두 가지이다. 하나는 현재의 응용 변환이 어떠한 다른 응용에도 노출되지 않는 것이고, 또 하나는 사용자가 각각의 새로운 응용에 대하여 그들의 생체정보를 재등록하는 불편과 수고 없이 새로운 응용에 대하여 기존의 등록을 사용할 수 있는 것이다.



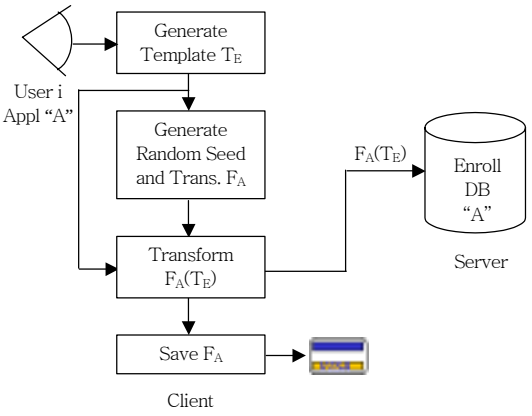
(그림 16) 생체정보 DB의 재생성

변환 기법의 또 다른 장점은, 만약 데이터베이스의 관리자가 생체정보의 손상 또는 포맷의 노출이 일어난 경우이거나 그러하다고 의심이 되면, 템플릿 권위자(Template Authority)가 전체 데이터베이스에 대하여 새로운 변환을 정의하여 포맷을 바꿈으로써 도난된 템플릿을 완전히 무효화하도록 요청할 수 있다. 이것은 패스워드가 유출되었을 경우 패스워드를 바꾸는 경우와 동일하다. 이 과정은 (그림 16)에 잘 나타나 있다. 즉, 응용 A로부터 새로운 포맷을 요청 받음에 따라 템플릿 권위자는 응용 A에 대한 새로운 변환 F_C를 생성한다. 권위자는 응용 A에 대하여 저장된 변환을 이용하여, 그의 역벽환을 취한 후 다시 F_C 를 적용하여 $F_C F_A^{-1}$ 을 생성한다. 이 변환은 응용 A의 데이터베이스 전체에 적용되어 등록된 템플릿들을 새로운 C 포맷으로 바꾼다. 동시에 사용자 변환도 A에서 C로의 포맷 변환을 반영하도록 수정 과정이 이루어져야 한다. 포맷의 개정 코드를 사용자가 제출한 템플릿에 통합하고, 쓸모없게 된 포맷이 탐지되었을 때 새로운 변환을 다운로드할 필요가 있다고 사용자에게 충고함으로써, 앞에서 기술한 수정 과정은 자동화 될 수 있다.

(그림 17)은 클라이언트-서버에서의 인증과정을 나타낸다. 우선 사용자가 응용 A에 대하여 이전에 이미 등록하여 데이터베이스 A가 등록 템플릿을 포함하고 있다고 가정한다. 사용자가 인증받기를 원할 때 그는 유일한 변환을 위하여 서버에 "시드(seed)"



(그림 17) 클라이언트-서버 인증과정 예



(그림 18) 클라이언트-서버 등록과정

넘버 또는 키에 대한 요청을 생성한다. 서버는 (그림 17)에서 "X"로 표기된 랜덤 시드를 생성하여 이를 클라이언트에 전송함과 동시에 (5)의 변환을 계산하여 임시 저장장소에 저장한다.

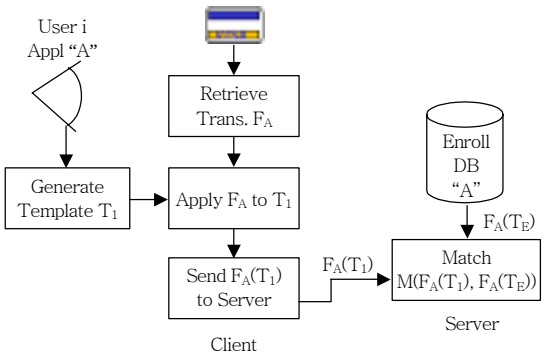
$$F_{X,A} = F_A F_X^{-1} \quad (5)$$

클라이언트는 전송받은 X를 이용하여 그 자신의 F_X를 생성한다. 그리고 영상을 캡처하고 F_X를 사용하여 루트 템플릿 T_1을 변환한다. 만약 원한다면 $Fx(T_1)$은 디지털 서명되고 암호화된 후 서버로 전송된다. 서버에서는 이 템플릿을 복호화하고 디지털 서명 기법을 이용하여 무결성을 검증한 후, 임시로 저장된 변환 $F_{X,A}$를 이용하여 (6)과 같이 클라이언트의 템플릿을 데이터베이스 A에 적합한 포맷으로 바꾼다.

$$F_A(T_1) = F_{X,A}(F_X(T_1)) = F_A F_X^{-1}(F_X(T_1)) \quad (6)$$

클라이언트의 템플릿은 이러한 한 번의 트랜잭션을 위하여 유일한 포맷으로 생성되어 서버로 전송된다. 그리고 서버만이 $F_X(T_1)$을 등록된 데이터베이스에 부합되게 하는 데 필요한 정보를 갖고 있다.

또 다른 클라이언트-서버 등록 및 인증과정을 (그림 18)과 (그림 19)에서 보여 준다. 이 경우도 역시 사용자가 응용 A에 대한 데이터베이스에 이미 등록되어 있다고 가정한다. 그러나 이 경우에는 등록이 수행되기 전에 클라이언트 응용프로그램에서 랜덤



(그림 19) 클라이언트-서버 인증과정

시드를 발생하여 (그림 17)에서와 같이 그 자신의 유일한 "A" 변환을 계산한다. 이 변환은 등록 템플릿에 적용하여 변환된 템플릿을 서버에 전송한다. 또한 이 변환은 사용자가 소유할 수 있는 스마트 카드 또는 휴대용 매체에 저장된다. 이제 사용자는 매번 휴대용 저장장치에 적절한 변환을 저장함으로써, 수많은 응용에 등록을 수행할 수도 있다. 또한 등록된 데이터베이스 내의 각 템플릿은 오직 사용자에게만 알려져 있는 그 자신의 유일한 포맷을 갖게 될 것이다. 따라서 생체 템플릿의 유일한 포맷이 휴대용 매체에 저장된 변환에 의하여 정의되기 때문에, 사용자는 그 자신의 생체 데이터를 완벽하게 통제할 수 있게 된다. 응용 "A"에 대한 인증이 요청되었을 때, 사용자는 적절한 생체 장치를 통하여 영상을 획득하여 루트 템플릿을 생성한 후, 응용 "A"에 대한

휴대용 매체를 적절한 리더에 삽입한다. 이러한 과정을 (그림 18)에 나타내었다. 클라이언트 응용프로그램에서 변환을 읽어들인 후, 이를 루트 템플릿에 적용하여 이 변환된 템플릿을 서버로 전송한다. 또한 변환된 템플릿은 서버로 전송되기 전에 암호화되고 디지털 서명화된다.

이와 같은 생체 템플릿을 변환하는 기법은 인증 기법의 정확도와 유연성을 유지하고, 생체 데이터베이스의 프라이버시를 보장하고, 소유자의 허가 하에 등록된 템플릿들의 재사용과 공유를 허용하고, 생체 템플릿이 손상되었을 경우에는 재발행을 할 수 있게 한다. 이러한 변환들은 생체인식에 있어서 프라이버시 보호에 대한 중요 이슈를 해결할 수 있고, 대용량 데이터베이스를 가진 인식 시스템에 장점을 주는 생체인식 기법을 제공할 수 있게 한다.

V. 맺음말

본 고에서는 생체인식 기술을 대규모 응용에 적용하기 위하여 필요한 생체정보의 안전한 저장/전송/처리 등 생체정보 보호에 대한 연구 동향을 살펴보았다. 생체정보를 이용한 본인 인증은 기존의 패스워드에 비해 많은 사용상의 장점을 가지고 있다. 즉, 사용자는 자신의 정보를 아무리 나이가 어린 아이일지라도 결코 분실하지는 않는다. 그러나 생체정보를 사용하는 시스템을 포함해서 어떠한 시스템이라도 미리 준비한 해커에 의한 공격에 대해서는 거의 무방비 상태일 수 있다. 전형적인 생체인증 시스템에서의 가능한 공격포인트를 8가지 정도로 분류해서 살펴보았다. 그리고 이를 방지하기 위한 몇 가지 정도의 방법에 대해서 살펴보았으며, 지속되는 공격에 대해서는 압축된 지문신호에 직접적으로 일정한 양의 표시를 첨부해서 사용하는 데이터 은닉 기술이나 센서로부터 얻어진 신호에 대한 생체 확인을 질의/응답 기법으로 해결할 수 있음을 살펴보았다. 마지막으로 가끔 간과할 수 있는 개인 프라이버시 문제와 생체정보의 무효화 문제를 살펴보았다.

생체인식의 가장 강력한 힘인 "시간의 흐름에도 변하지 않는다"는 것이 오히려 가장 큰 문제가 될 수 있다는 사실은 참으로 역설적인 사실이 아닐 수 없다. 먼저 다른 생체 정보를 사용하고자 하더라도 개인이 가지고 있는 사용가능한 생체정보에는 한계가 있다. 예를 들어, 10개의 손가락, 2개의 눈, 1개의 얼굴, 2개의 손 등으로는 한계가 있다. 따라서 일단 생체정보가 도용되면 이는 더 이상 바꿀 수 없다는 문제가 있다(Once compromised, compromised forever). 이와 같은 문제를 해결하기 위하여 생체정보에 반복사용이 가능하고 복구가 불가능한 변형법을 적용하는 것이다. 무효화는 단순히 새로운 distortion 함수를 사용하면 가능하다. 아울러 개인의 프라이버시 문제도 한층 더 강화될 수 있다. 왜냐하면 서로 다른 서비스나 응용 분야에 대해서 서로 다른 변형 함수를 사용하기 때문이며(Different distortions for different accounts), 실제 생체정보는 저장되지 않을 뿐 아니라 나타나지도 않기 때문이다.

참 고 문 헌

[1] B. Schneier, "The Uses and Abuses of Biometrics," *Communications of the ACM*, Vol. 42, No, 8, 1999, p. 136.

[2] N. Ratha, J. Connell, and R. Bolle, "An Analysis of Minutiae Matching Strength," *Proc. of AVBPA 2001 (LNCS 2091)*, 2001.

[3] T. Matsumoto et al., "Impact of Artificial Gummy Fingers on Fingerprint Systems," *Optical Security and Counterfeit Deterrence Technique*, Vol. 4673, 2002, pp. 275-228.

[4] N. Ratha, J. Connell, and R. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems," *IBM Systems Journal*, Vol. 40, No. 3, 2001, pp. 614-634.

[5] M. Yeung and S. Pankanti, "Verification Watermarks on Fingerprint Recognition and Retrieval," *Journal of Electronic Imaging*, Vol. 9, No. 4, 2002, pp. 468-476.

[6] A. Jain, U. Uludag, and R. Hsu, "Hiding a Face in a Fingerprint Image," *Proc. of ICPR*, 2002, pp. 756-759.

[7] B. Gunsel, U. Uludag, and A. Tekalp, "Robust Wa-

termarking of Fingerprint Images," *Pattern Recognition*, Vol. 35, 2002, pp. 2739-2747.

[8] A. Jain and U. Uludag, "Hiding Fingerprint Minutiae in Images," *Proc. of AutoID*, 2002, pp. 97-102.

[9] A. Jain, U. Uludag, and R. Hsu, "Hiding a Face in a Fingerprint Image," *Proc. of CPR*, 2002, pp. 756-759.

[10] N. Ratha, J. Connell, and R. Bolle, "Secure Data Hiding in Wavelet Compressed Fingerprint Images," *Proc. of Multimedia*, 2000, pp. 127-130.

[11] N. Ratha, J. Connell, and R. Bolle, "Cancelable Biometrics," *Biometric Consortium*, 2000.

[12] J. Cambier and M. Braithwaite et al., "Application-Specific Biometric Templates," *Proc. of AutoID*, 2002, pp. 167-171.